D4 E1
Contd

decrypting said transmitted encrypted software code at the one GSP unit according to said GSP unit unique software key used to encrypt the software code by the supplier; and

replacing the prior software code at the one GSP unit with the decrypted software code from the supplier.

Amd
F2

26. (New Claim) The method in accordance with claim 25 wherein said step of encrypting the software code includes using cyclic redundancy coding.

27. (New Claim) The method in accordance with claim 26 wherein said step of encrypting the software code uses the GPS unit software key as a seed.

28. (New Claim) The method in accordance with claim 26 wherein the encrypted software code transmitted by the supplier includes a footer tag that includes the GPS unit software key.

29. (New Claim) The method of claim 28 wherein said step of decrypting said transmitted software code comprises reading the GPS unit software key from the footer tag and comparing the software key in the footer tag with the software key of the GPS unit.

REMARKS

The specification is being amended to correct minor grammatical errors and the duplication of reference numeral 40. A corrected Fig. 6 is also attached for the Examiner's review and approval wherein the database in Fig. 6 is identified by reference numeral 39, whereas the Product in Fig. 5 remains identified by reference numeral 40.

In the Office Action being responded to the Examiner has rejected all of the prior claims 3-25 as anticipated by Wasilewski et al patent 5,341,425, 35 USC 102(e) or unpatentable over Wasilewski et al in view of Teare et al patent 5,243,652 , 35 USC 103(a). The Teare et al patent discloses a Global Positioning System 10 which communicates with a central facility 12. The central facility, on the basis of the location of the remote node as compared with a list of predetermined locations in its database, will send a decryption key to the node 11 which will enable the node to decode an encrypted signal being sent to the node. As discussed below, this is distinct from applicants' invention, both as to the problem to be solved by applicants' invention and their inventive solution.

Wasilewski et al, the Examiner's primary reference, is directed to transmitting encrypted data from a plurality of transmission sites to a single reception site, each of the transmission sites having both a unique broadcast key for the site as well as a common system key. The reception site has stored in a memory both its system key and the broadcast key of each of the transmission sites. Unlike applicants' invention, the transmission of data is from the remote transmission sites to the central reception site. This is, of course, directly contrary to applicants' invention and is neither a disclosure or a teaching of applicants' invention, as set forth in the newly presented claims.

Applicants' invention, as now more precisely recited in the newly presented claims, is directed to providing new or replacement software code from a ground software supplier or vendor. The software supplier or vendor does not have stored any unique key for the GPS unit which is to have the new software. In accordance with applicants' invention, one step is for the GPS unit which has assigned to it a unique software key to forward " a request for the updated aeronautical software data to a software supplier, said request including the GPS unit unique software key and payment authorization information," to quote the language of newly presented claim 15.

In response to the Examiner's comments with respect o the prior claims, the Examiner's paragraph 13, newly presented claim 25 now clearly sets forth that the method is applied in the environment where there are a plurality of GPS units, each in an aircraft. Further, with reference to the Examiner's noting that the performance of the example at page 3 of applicants' specification was not required by the prior claims, newly presented claim 25 specifically recites that the request for the updated aeronautical navigation data include both the GPS unit unique software key and payment authorization information.

In neither of the references is there any suggestion of a supplier encrypting software code for updated aeronautical navigation data, the encrypted software code including a decryption program, and transmitting the decryption program which only allows software to be unloaded by the GPS unit out of the plurality of GPS units having the unique software key, which key is then used by that GPS to decrypt the software code provided by the supplier and to replace the prior code with the now decrypted software code from the supplier.

New dependent claims 26 to 29 further characterize various of the unique steps of applicants' inventive method, as set forth in the new independent claim 25.

Applicants in their description of the prior art, at page 1, line 20 et seq of their specification, have set forth some of the problems related to providing updated navigation data to a GPS unit in an aircraft. Neither Wasilewski et al nor Teare et al, either singly or in combination, anticipate or suggest applicants' novel and inventive solution to these problems, as set forth in the newly presented claims.

Favorable consideration and allowance of new claims 25 to 29 and passage of this application to issue are therefore respectfully requested.

CONCLUSION

The claims now being in form for allowance, reconsideration and allowance is respectfully requested. If the Examiner has questions or wishes to discuss any aspect of the case, the Examiner is encouraged to contact the undersigned at the telephone number given below.

Respectfully submitted,

Agent:
Eric G. Halsne
Registration No.: 46,753
Date: November 12, 2001 (Monday)
Post Office Address: Honeywell Int'l Inc.
101 Columbia Road
P.O. Box 2245
Morristown, NJ 07962
Phone Number: (425) 376-2107

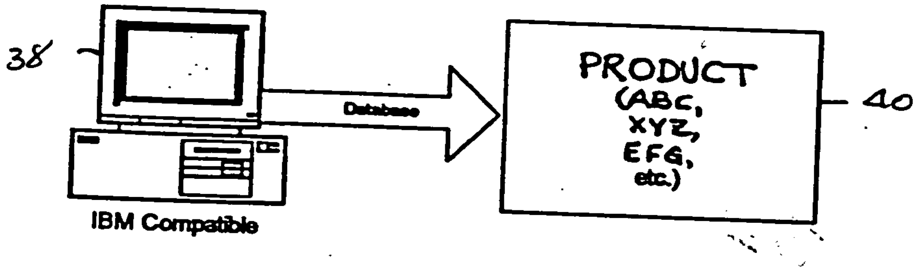
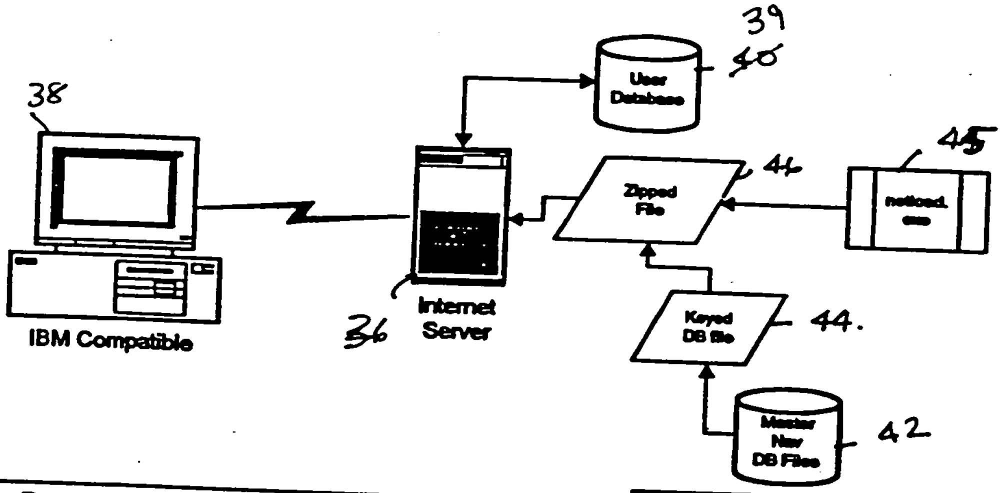


FIG. 5



User Provides:

1) Choice of Database
2a) Credit Card Number OR
2b) Account name & password*
3) Database Key

* - User has already set up an account with (SELLER) before calling if account/password option is used.

SELLER PERFORMS:

1a) Credit-card check OR
1b) Account/Password verification
2) Stamp a master DB file with key
3) Create a .zip file with key-ed DB file and netload.exe software
4) Download the .zip file to the user
5) Charge the user's credit card

FIG 6.

Mark-up Copy

database, to provide an indication of the vehicle or aircraft relative to the topographical data or highway information. For example, as disclosed in U.S. Patent Application Serial No. 08/509,642 filed on July 31, 1995, assigned to the same assignee of the present invention, the topographical data, such as the elevation of the highest obstacles within a predetermined region, are stored in a memory device aboard the aircraft. The GPS allows the topographical data to be displayed as a function of the position of the aircraft.

Often times, the topographical and navigational data needs to be updated due to changing topography and highway information. Because of the relative ease in which software that is transmitted over the Internet can be duplicated, updates of the topographical data ~~is~~ are known to be provided in a diskette or cartridge form and mailed to the customers. Typically, users of such integrated GPS systems must first determine if an update is available by checking with the database vendor. Orders are typically placed by telephone. The update diskette or cartridge is then mailed to the customer. As such, from the time the order is placed, considerable time passes before the updated topographical data is actually received by the customer so it can be uploaded into the customer's integrated GPS unit. The delay is even more acute for international customers for which the mailing time is considerably greater.

There are other problems associated with providing updated topographical and navigational data on diskettes or cartridges to a customer. For example, for customers that have multiple integrated GPS units, the customer may choose to upload the updated data onto such multiple units even though the customer has only paid for the update for a single unit. The customer may also transfer the update diskette or cartridge to another unauthorized user.

Mark-up Copy

The software layout for the system is illustrated in FIG. 6 and includes a user database ~~40~~ 39, a master "nav" database 42 and an upload program 44, identified as NETLOAD.EXE. The user information for example, regarding account and password information, etc. is maintained in the user database ~~40~~ 39, accessible by the server 36. The topographical information is stored in the master "nav" database file 42, also accessible by the server 36. Once the user provides the unique software key as well as the desired payment method, a copy of the topographical and/or navigation data from a master "nav" file 42 is encrypted as a function of the unique software key, provided by the user and stored in a "keyed DB file" 44. The keyed DB file 44 is then compressed into a zip file 46 and transferred to the user by way of the Internet along with the decryption or upload file 44, identified as NETLOAD.EXE. The decryption file 44 enables the zip file containing the encrypted database to be uploaded into a product 40 as long as the software key of the product matches the software key to which the database was encrypted. If the software key matches the unique key within the product, the database is decrypted and uploaded into the product.

A simplified flowchart for the system in accordance with the present invention is illustrated in FIG. 7. Initially, the user connects to the database vendor's home page in step 48. Once connected to the database vendor's home page, the user selects a database from the available databases in step 50. Steps 52 and 54 provide for alternate payment methods. If a user wishes to avoid providing credit information over the Internet, the user can obtain a password and an account and become a registered user. Thus, the system checks whether the user is a registered user in step 52. If not, the system assumes the payment will be made by

Marked-up copy

including the software key from the encrypted output file 82. As discussed in more detail below, the software key from the footer tag is used to decrypt the first byte of the database in step 88. After the first byte is decrypted, the key is updated for the next byte in step 90. After the new key is updated, a checksum is calculated to determine if there are any errors in the data in step 92. The process of steps 88-92 is repeated for each byte in the encrypted database file 82, as indicated by step 94. After all of the bytes in the output file 82 have been decrypted, the system checks in step 96 to determine whether the checksum for the decrypted file matches the original checksum included in the footer tag in the output file 82 in step 96. If there are any discrepancies in the checksum, an error message is displayed in step 98. If the checksums match, the system communicates with the GPS unit 40 in step 98 and awaits for the GPS unit 40 to send an identification packet containing the GPS unit type as well as the software key. Once the software key and GPS unit type are received from the GPS unit 40, the system determines in step 100 whether the GPS unit type matches the database file requested. If not, an error message is displayed in step 102. Otherwise, the system proceeds to step 104 and ascertains whether the software key received from the GPS unit 40 matches the software key used to encrypt the database file and contained in the footer tag mentioned above. If not, an error message is displayed in step 106. Otherwise, the system proceeds to step 108 where the software key received from the GPS unit is used to decrypt the first byte in the output file 82. After the first byte is decrypted or unkeyed, the key is updated in step 110 for the next byte. The steps 108 and 110 are repeated until a sufficient number of bytes have been unkeyed for a full packet as indicated in step 112. Each time a packet is